

# Password Security

According to IBM's 2023 Cost of Data Breach Report, compromised or stolen credentials emerged as one of the primary initial attack vectors, accounting for 15% of breaches in 2023.

## USE A PASSWORD MANAGER



The average person must remember between 70-80 passwords. A password manager is a digital vault that stores, secures and presents a password when a user logs in, so you don't have to remember the password.

**45m** people rely on password managers

(Security.org, 2023)

**51%** of employees share passwords with co-workers

(Yubico and Ponemon)

## NEVER SHARE YOUR PASSWORD

Sharing passwords means that those passwords are out of your control. Control is critical in maintaining security. You should never share your passwords or write them down.

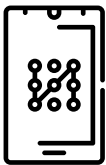


## USE MULTI-FACTOR AUTHENTICATION

Even the strongest password can't protect your account if it gets compromised in a data breach. Two-factor authentication, also known as 2FA, adds an extra layer of security to your online accounts.



## DON'T REUSE PASSWORDS



To ensure you remain safe and secure, always use a password that is unique to each of your accounts.

**84%** of people use the same password across multiple accounts

(Bitwarden survey)

## DON'T USE PERSONAL INFORMATION

A password should never include basic information about yourself, such as the names of relatives, dates of birth or pet names.



The most popular password is  
**123456**

## MAKE PASSWORDS HARD TO GUESS

Using a popular password makes the cybercriminal's job easier. A strong password should be unpredictable, composed of a mix of uppercase and lowercase, more than ten characters long, and contain numbers and special characters.

